Bescherming persoonsgegevens is PET

Koops, E.J.

Published in:
Nieuwsbrief IT & Recht

Publication date:
1996

Koops, B.J. (1996), 'Bescherming persoonsgegevens is PET', Verschenen in:
IT&Recht 1 (1), 6-7

Bescherming persoonsgegevens is PET

Als je aan de apotheek zegt dat je stopt met de pil, krijg je na negen maanden een aanbieding voor geweldige luiers in de bus. Koop je regelmatig wat bij de juwelier, dan wil de fiscus weten waar je dat geld vandaan haalt. En als je Airmiles spaart, krijg je iemand op de stoep met een wandkleed dat precies in je interieur past. Is dat de informatiemaatschappij waarin we willen leven? De Registratiekamer vindt van niet.

De Nederlandse privacy-waakhond bepleit een cultuuromslag. Het bedrijfsleven moet niet uitgaan van het verzamelen van zoveel mogelijk persoonlijke gegevens maar van de bescherming van de persoonlijke levenssfeer. De consument heeft recht op privacy. Hij eist dat niet teveel gegevens over hem rondslingeren en hij zal daar zijn koopgedrag op afstemmen, verwacht de Registratiekamer. Het onlangs verschenen rapport "Privacy-enhancing Technologies" vertelt hoe nieuwe technologie de privacy adequaat kan beschermen.

pseudo-identiteit

De vlucht van de informatietechnologie bedreigt de privacy. Overal worden persoonsgegevens opgeslagen. Door koppeling van verschillende bestanden kan een zeer exact beeld ontstaan van iemands persoonlijke leven en levensstijl. Dit kan bedreigend zijn voor bijvoorbeeld patiënten, werknemers of mensen met een apart leefpatroon. Iedereen heeft een grondwettelijk recht op bescherming van de privacy, dat verder is uitgewerkt in bijvoorbeeld de Wet Persoonsregistraties en de recente Europese richtlijn bescherming persoonsgegevens (zie p...). Maar geven deze wetten in de praktijk wel voldoende bescherming?

Het blijkt dat het bedrijfsleven, waaronder IT-producenten en -aanbieders, nauwelijks oog heeft voor bescherming van persoonsgegevens, aldus het rapport van de Registratiekamer, dat in samenwerking met collega's uit Ontario (Canada) tot stand kwam. Veel bedrijven blijken wel oog te hebben voor de beveiliging van gegevens (met name integriteit en authenticiteit), maar als het gaat om het afschermen van de identiteit van gebruikers geven de meeste niet thuis.

Voor de meeste toepassingen is het helemaal niet nodig om de *identiteit* (naam, adres, functie) van gebruikers te kennen. Meestal volstaat een *pseudo-identiteit* net zo goed: de gebruiker krijgt voor elke specifieke toepassing een pseudoniem, bijvoorbeeld een bepaald nummer dat niet herleidbaar is tot de persoon zelf. Daarmee kan een IT-systeem net zo goed checken of iemand recht heeft op een bepaalde dienst. Alleen voor het autoriseren (het invoeren van iemands rechten in een systeem) en voor het afrekenen (het betalen van de dienst) moet de dienstaanbieder de identiteit van de gebruiker kennen. Een belangrijk deel van het proces van IT-gebruik kan dus afgeschermd worden tegen onnodig gebruik van persoonsgegevens.

chipkaart

Een voorbeeld. Bij het huidige betalingsverkeer weten banken precies welke transacties hun cliënten uitvoeren. Dat is gevoelige informatie. PET (Privacy-Enhancing Technologies) kunnen de risico's die daarmee samenhangen sterk terugbrengen. De bank zou kunnen werken met

pseudo-rekeningnummers die niet te herleiden zijn tot de klanten. De relatie tussen de identiteit van de cliënten en de pseudonummers wordt beheerd door een betrouwbare instantie (een Trusted Third Party (TTP) die het vertrouwen geniet van zowel de bank als de klanten); dit kan eventueel ook een kleine, afgeschermde eenheid binnen de bank zijn. De TTP vertaalt de "pseudo"-rekeningafschriften in gewone afschriften en stuurt deze naar de klanten. Ook geeft deze instantie de klant een chipkaart met zijn pseudo-nummer, dat is ondertekend met de digitale handtekening van de TTP. Winkels weten dan dat de klant inderdaad een rekening bij de bank heeft. De klant kan gewoon elektronisch betalen, zonder dat de bank of de winkel kan achterhalen wie de klant is. Alleen in geval van fraude kan de bank de TTP vragen wie achter het pseudonummer zit; daarover kunnen alle partijen vooraf onderlinge afspraken maken.

Een ander voorbeeld uit het rapport is rekeningrijden. Dat kan via betaling achteraf en via betaling vooraf. Bij betaling *achteraf* moet een tolsysteem registreren wie waar gereden heeft en vervolgens de rekening sturen naar de eigenaar van het kenteken. Daarbij is weinig bescherming mogelijk: het systeem slaat precies op waar je wanneer gereden hebt. Bij betaling *vooraf* kun je wel, zoals nu, anoniem blijven rijden. Je zet (anoniem) bij een pompstation digitaal geld op een chipkaart, die je in een apparaatje op de voorruit stopt dat kan communiceren met een tolapparaat. Het tolapparaat schrijft bij een tolgrens automatisch een bedrag af van de chipkaart. Je zou zo'n chipkaart voor meer dingen kunnen gebruiken, bijvoorbeeld als chipknip of als digitaal rijbewijs, maar daarbij moet worden voorkomen dat de combinatie van toepassingen weer extra persoonsgegevens kan opleveren. Op de chipkaart valt dat te scheiden door aan elke toepassing een andere pseudo-identiteit te koppelen en de toegang tot elke pseudo-identiteit af te schermen.

cultuuromslag

Technisch gesproken is heel veel mogelijk. De bescherming van persoonsgegevens hangt dan ook niet af van de techniek, maar van de wil van het bedrijfsleven. Zij moeten zich bewust zijn van de noodzaak om zorgvuldig om te gaan met persoonsgegevens. Ontwikkelaars van IT-produkten moeten al in de ontwerpfase het domein waar de identiteit van de gebruiker bekend is zoveel mogelijk beperken. Het pseudo-domein, waar de gebruiker alleen onder een pseudoniem bekend is, kan dan zo groot mogelijk zijn.

[afbeelding: Figure 4.5, p. 26 deel II)

Het probleem is dat er in de praktijk nauwelijks aandacht is voor privacybescherming. De Registratiekamer ziet het dan ook als grootste uitdaging het bedrijfsleven zover te krijgen dat ze al bij het ontwerpen en in gebruik nemen van IT-produkten rekening houden met de privacy van de gebruikers. Daarvoor is een heuse cultuuromslag nodig en die zal niet makkelijk zijn. Maar het rapport is optimistisch. Consumenten zullen kritischer worden over de opslag van persoonsgegevens. Ze zullen eisen dat IT-diensten en -produkten zoveel mogelijk anoniem zijn. Het is aan het bedrijfsleven om daarop in te spelen. Dan hoef je tenminste geen luiers te gaan gebruiken als je toevallig overstapt van de pil op condooms.

Bert-Jaap Koops is onderzoeker in Tilburg en Eindhoven.

Koops, B.J. (1996), 'Bescherming persoonsgegevens is PET', Verschenen in: *IT&Recht 1* (1), 6-7

Registratiekamer, Information & Privacy Commissioner (Ontario), *Privacy-enhancing Technologies: The path to anonymity*, ISBN 90 346 32 024, te bestellen bij SDU DOP, 070-3789830.